

BALTIMORE SUN
22 November 1985

9A.

ESPIONAGE

Codes protected poorly, Pentagon panel warns

By Vernon A. Guidry Jr.
Washington Bureau of The Sun

WASHINGTON — Although U.S. military codes and coding apparatus are among the most important secrets an enemy could steal, the armed services have no special controls to keep them secret, a Pentagon commission said yesterday.

"There are no special eligibility criteria for personnel handling cryptographic materials despite their transcendent importance to an adversary," according to a report of the commission appointed to study security issues in the wake of the Walker spy case. "Only those individuals who have access to nuclear weapons are currently monitored formally for trustworthiness and stability."

While "crypto," or code, material is subject to normal classification procedures, the panel found those procedures inadequate. "Cryptographic information continues to have crucial significance inasmuch as its compromise to hostile intelligence services can, in turn, lead to the compromise of any classified information being transmitted over secure voice or secure data channels," the panel's report said.

The panel said that a special access program for cryptographic work should be established, limiting it to U.S. citizens and making access dependent on willingness to take a lie-detector test.

That was one of a number of security recommendations in the report made public yesterday.

Only one of the recommendations by the panel, which was appointed by Defense Secretary Caspar W. Weinberger, prompted immediate action. Mr. Weinberger ordered a one-time, "top-to-bottom" security inspection of all armed forces and Pentagon civilian operations that handle classified information. He told the services and the civilian defense agencies to report back to him by Oct. 1, 1986, with an overall assessment of security for classified information and recommendations for any further steps needed to safeguard it.

Robert B. Sims, spokesman for the secretary, said Mr. Weinberger "indicated general endorsement" of the panel's report and would consid-

er the other recommendations individually.

The commission said that overall Pentagon performance in adhering to existing security regulations "must be considered uneven at best."

While saying that it was hard to determine how damaging lax enforcement might be, the panel found examples of such laxity.

"Some commanders and supervisors show a clear disdain for security, leaving compliance to clerks and secretaries. When security requirements become an impediment, they are ignored either for reasons of personal convenience, or to facilitate job performance," the report said.

The panel made no explicit mention of the Walker spy case. A former Navy warrant officer, John A. Walker Jr., and his sailor son, Michael, have pleaded guilty to espionage. John Walker's brother, Arthur, has been convicted of spying, and a fourth man awaits trial on the West Coast on charges of spying for Walker and Moscow.

The chief damage the spy ring is said to have caused involves passing Navy codes and code-making apparatus to the Soviet Union.

Retired Army Gen. Richard G. Stilwell, head of the panel, told reporters yesterday that he believed that had a special scrutiny crypto program been in place, the spies might have been deterred, or at least caught sooner. The Walker ring is said to have operated for nearly 20 years.

More generally, the panel said the Pentagon must put more money and effort into information security "even at the expense of other . . . programs." The department "must be willing to pay a higher price, in terms of both resources and operational convenience, to protect its classified information," the report concluded.

It echoed other critics on such issues as permitting too many security clearances and conducting too few investigations and re-investigations of security-clearance holders. It also pointed out that there was little or no research on the psychological and behavioral aspects of human security problems.